PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-308564
(43)Date of publication of application : 05.11.1999

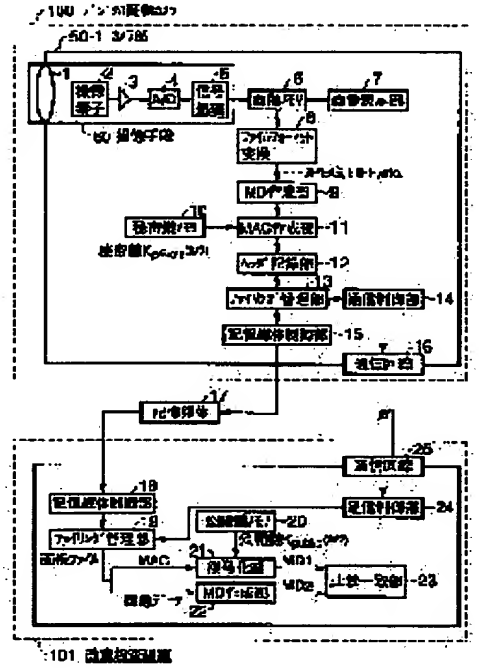
(51)Int.Cl. H04N 5/91
G09C 5/00
H04N 5/765
H04N 5/781
H04N 5/92

(21)Application number : 10-109352
(22)Date of filing : 20.04.1998

(71)Applicant : OLYMPUS OPTICAL CO LTD
(72)Inventor : KONDO TAKASHI
HIGURE MASAKI
KOMIYA YASUHIRO
YAMADA HIDETOSHI

(54) DIGITAL EVIDENCE CAMERA SYSTEM, DECODING KEY ACQUISITION REGISTRATION SYSTEM AND DIGITAL IMAGE EDIT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a digital evidence camera system where evidence capability of a digital image is enhanced and an encrypted key is managed at a very high security level.
SOLUTION: The digital evidence camera system detects falsified image data obtained by photographing an object with a camera and consists of a camera section 50-1 provided with an image pickup means 60 that photographs an object and with a MAC generating section 11 that generates falsification detection data (MAC) from image data by photographing by using a secret key set in advance and of a falsification check device 101 that uses a public key corresponding to the secret key to decode the data MAC and checks whether or not the image data are falsified based on the decoding result.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] The image pck-up section for being the digital of-evidence camera system which detects an alteration of the image data which picturizes a photographic subject with a camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pck-up using the encryption key built in beforehand, the camera which ******s, and the alteration detection section which detects whether the aforementioned data for alteration detection are decrypted using the decryption key corresponding to the aforementioned encryption key, and the aforementioned image data was altered based on the result of this decryption -- since -- the digital of-evidence camera system characterized by becoming
[Claim 2] The image pck-up section for being the digital of-evidence camera system which detects an alteration of the image data which picturizes a photographic subject with a camera and was obtained, and picturizing a photographic subject, The cipher-processing section which creates the data for alteration detection from the image data obtained by the image pck-up using the encryption key built in beforehand, The camera which ******s, and the alteration detection section which detects whether the aforementioned data for alteration detection are decrypted using the decryption key corresponding to the aforementioned encryption key, and the aforementioned image data was altered based on the result of this decryption, since -- the alteration supervision mode as which, as for the aforementioned camera, the aforementioned image data detects whether it was altered or not -- in addition, with the secure mode in which encryption to the image data transmitted to the aforementioned alteration detection section from the aforementioned camera is performed It has the digital-watermarking mode which embeds digital-watermarking data at image data, and the normal mode which performs usual photography without working a security function. The digital of-evidence camera system characterized by having the mode selection section for choosing the mode of at least one request from these modes.
[Claim 3] The decryption key storage section memorized in accordance with an identifier peculiar to equipment, and the 1st decryption key corresponding to the 1st encryption key generated corresponding to this identifier, The decryption key output section which creates the data for alteration detection about the decryption key of the above 1st using the 2nd encryption key, and is outputted in accordance with this data for alteration detection, and the decryption key of the above 1st, A ********** server and the decryption key storage section which memorizes the decryption key of the above 1st acquired from the aforementioned decryption key server through means of communications etc., The aforementioned data for alteration detection supplied from the aforementioned decryption key server through means of communications etc. are decrypted using the 2nd decryption key corresponding to the encryption key of the above 2nd. the decryption key acquisition section equipped with the alteration detection section which detects whether the decryption key of the above 1st was altered based on the result of this decryption -- since -- decryption key acquisition / registration system characterized by becoming
[Claim 4] With the filing Management Department which does the filing management of the image data which is the digital picture image edit system into which image data is edited, and was inputted through the picture image input section while the alteration of image data was detected While the 1st data for alteration detection beforehand given to the aforementioned image data is decrypted using the decryption key corresponding to the encryption key used when creating this data for alteration detection The alteration detection section which detects the alteration status of image data by comparing this the 1st data for alteration detection and aforementioned image data by which decode was carried out, To the aforementioned image data from the edited image data to which various image processings were performed by the picture image editorial department which performs various kinds of image processings, and the aforementioned picture image editorial department, and the data of the edit history by the aforementioned picture image editorial department the update section of an image file which creates the 2nd data for alteration detection using the encryption key other than the aforementioned encryption key, and adds this to the aforementioned edited image data -- since -- the digital picture image edit system characterized by becoming

---

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－308564

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｎ	5/91		Ｈ０４Ｎ	5/91	Ｊ
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
Ｈ０４Ｎ	5/765		Ｈ０４Ｎ	5/781	５１０Ｊ
	5/781			5/92	Ｈ
	5/92				

審査請求　未請求　請求項の数４　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－109352

(22)出願日　平成10年(1998)４月20日

(71)出願人　000000376
オリンパス光学工業株式会社
東京都渋谷区幡ヶ谷２丁目43番２号

(72)発明者　近藤　隆
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内

(72)発明者　日暮　正樹
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内

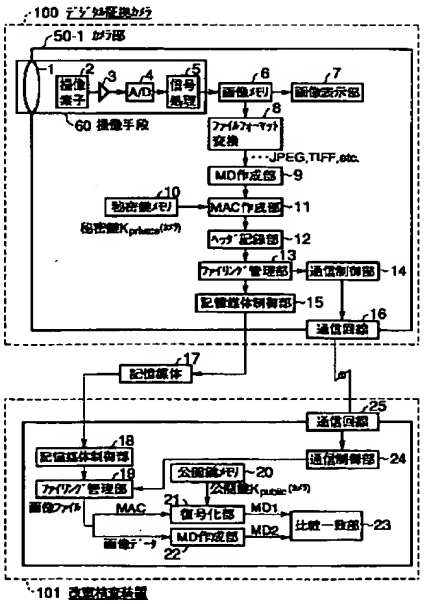
(72)発明者　小宮　康宏
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内

(74)代理人　弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　デジタル証拠カメラシステム、復号化鍵取得・登録システム、及びデジタル画像編集システム

(57)【要約】
【課題】デジタル画像の証拠能力を高めて、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステムを提供する。
【解決手段】カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像手段６０と、撮像により得られた画像データから、あらかじめ内蔵された秘密鍵を用いて改竄検知用データ（ＭＡＣ）を作成するＭＡＣ作成部１１とを具備するカメラ部５０－１と、秘密鍵に対応する公開鍵を用いてＭＡＣを復号化し、この復号化の結果に基づいて画像データが改竄されたか否かを検知する改竄検査装置１０１とからなる。



1

【特許請求の範囲】

【請求項１】　カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、

被写体を撮像するための撮像部と、

撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、

を具備するカメラと、

前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、

からなることを特徴とするデジタル証拠カメラシステム。

【請求項２】　カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、

被写体を撮像するための撮像部と、

撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、

を具備するカメラと、

前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、

からなり、

前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも１つの所望のモードを選択するためのモード選択部を有することを特徴とするデジタル証拠カメラシステム。

【請求項３】　装置に固有の識別子と、この識別子に対応して生成された第１の暗号化鍵に対応する第１の復号化鍵とをあわせて記憶する復号化鍵記憶部と、

前記第１の復号化鍵に関する改竄検知用データを第２の暗号化鍵を用いて作成し、この改竄検知用データと前記第１の復号化鍵とをあわせて出力する復号化鍵出力部と、

を備えた復号化鍵サーバと、

前記復号化鍵サーバから通信手段等を介して取得した前記第１の復号化鍵を記憶する復号化鍵記憶部と、

前記第２の暗号化鍵に対応する第２の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化し、この復号化の結果に基づいて前記第１の復号化鍵が改竄されたか否かを検知する改竄検知部と、

を備えた復号化鍵取得部と、

からなることを特徴とする復号化鍵取得・登録システム。

2

【請求項４】　画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、

画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、

前記画像データにあらかじめ付与された第１の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第１の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、

前記画像データに対し、各種の画像処理を施す画像編集部と、

前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第２の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部と、

からなることを特徴とするデジタル画像編集システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル証拠カメラシステム、復号化鍵取得・登録システム、及びデジタル画像編集システムに関する。

【０００２】

【従来の技術】従来、例えば、カメラのフィルムやメディアにアナログで記録された写真や音声は、裁判等において証明力のあるものとして用いられている。近年のデジタル技術の進歩により、画像や音声をデジタルデータとして記録する装置が普及している。このようなデジタル化によれば、コピーしても劣化しない、通信回線を使って素早く配布できる、さらに情報内容の加工・編集を容易に行えるという長所が得られる。しかし、加工・編集が容易であるということは、一方で情報内容を容易に改竄できるということであり、情報として証拠能力が疑われる余地が生まれる。したがって、デジタルの画像や音声を証拠品として使えるようにするためには、なんらかの方法でデジタルデータの改竄を防止する機能を備えていることが必要である。このような防止機能を有するカメラはデジタル証拠カメラと呼ばれている。

【０００３】このデジタル証拠カメラを実現するために、一般に通信等で用いられている電子署名技術を応用することが考えられている。電子署名システムでは、対となる２つの鍵が用いられる。１つは、暗号化のための鍵で秘密鍵と呼ばれ、もう一方は復号化のための鍵で公

開鍵と呼ばれる。デジタルデータは秘密鍵を用いて暗号化され、公開鍵を用いて復号化される。秘密鍵から公開鍵を求めるには一方向性関数が用いられるが、この一方向性関数の性質により、逆に公開鍵から秘密鍵を求めることは数学的に非常に難しいものとなっている。秘密鍵は持ち主以外の人が絶対に使えないように厳重に管理される必要がある一方、公開鍵は誰でも使えるように一般に公開される。

【０００４】改竄検知の方法は、送信側で、まず対象のデジタルデータからハッシュ関数などを使って、メッセージ・ダイジェスト（Message　Digest、以下、ＭＤ）と呼ばれるコードを作成する。対象のデジタルデータからＭＤを抽出する方法は公開されており、オリジナルデータがあれば誰でもＭＤを抽出することはできる。ちなみに、ＭＤはハッシュ関数の良く知られた性質から元のデジタルデータが少しでも異なると値が大きく変化するという性質がある。

【０００５】次に抽出されたＭＤを秘密鍵を用いて暗号化し、これをメッセージ認証子(Message Authentication　Code、以下、ＭＡＣ）として、オリジナルデータとともに相手側に送信する。ここで、秘密鍵と対となる公開鍵は受信者に確実に渡されているものとする（受信者が必ずその鍵を手にいれていればよく、第３者の手に渡ってもかまわない）。

【０００６】受信側は、オリジナルデータが改竄されていないことを調べるために、まず、オリジナルデータからハッシュ関数などを用いてＭＤ’を求める。次に公開鍵を用いてＭＡＣを復号化してＭＤを求め、このＭＤとＭＤ’とが一致するかどうかを調べる。もし、オリジナルデータが第３者によって改竄されたとしても、第３者は秘密鍵を持っていないので、公開鍵で復号化できるＭＡＣを作成できず、ＭＤとＭＤ’とは異なる値となる。これによって、オリジナルデータが第３者によって改竄されたことがわかる。

【０００７】

【発明が解決しようとする課題】上記したように、デジタルデータの改竄を検知するために電子署名技術を応用することができる。しかしながら、上記したような改竄検知の方法をデジタル証拠カメラに採用した場合、暗号化鍵としての秘密鍵は絶対漏洩することがあってはならないが、従来はこの秘密鍵を高いセキュリティレベルで管理することが容易でなく、したがって、デジタル画像の証拠能力を高めることができなかった。

【０００８】また、画像の場合にはデータの性質上、データ圧縮や領域切り出し、キャプションの挿入等の処理を施す必要のある場合が多いが、従来、文書データに対して応用されている電子署名の方法では、データ内容が僅かでも変更すると、データが改竄されたと見なされてしまう。したがって、従来の電子署名システムでは、上記のような画像データの性質上必要な編集が一切できなかった。

【０００９】本発明はこのような課題に着目してなされたものであり、その目的とするところは、デジタル画像の証拠能力を高めることができ、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステム、復号化鍵取得・登録システムを提供することであり、さらに画像の性質上必要となる圧縮や領域切り出し、キャプションの挿入等の編集を施してもデジタル画像の証拠能力を保てるデジタル画像編集システムを提供することにある。

【００１０】

【課題を解決するための手段】上記の目的を達成するために、第１の発明は、カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部とからなる。

【００１１】また、第２の発明は、カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部とからなり、前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも１つの所望のモードを選択するためのモード選択部を有する。

【００１２】また、第３の発明は、復号化鍵取得・登録システムであって、装置に固有の識別子と、この識別子に対応して生成された第１の暗号化鍵に対応する第１の復号化鍵とをあわせて記憶する復号化鍵記憶部と、前記第１の復号化鍵に関する改竄検知用データを第２の暗号化鍵を用いて作成し、この改竄検知用データと前記第１の復号化鍵とをあわせて出力する復号化鍵出力部と、を備えた復号化鍵サーバと、前記復号化鍵サーバから通信手段等を介して取得した前記第１の復号化鍵を記憶する復号化鍵記憶部と、前記第２の暗号化鍵に対応する第２の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化

し、この復号化の結果に基づいて前記第１の復号化鍵が改竄されたか否かを検知する改竄検知部と、を備えた復号化鍵取得部とからなる。

【００１３】また、第４の発明は、画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、前記画像データにあらかじめ付与された第１の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第１の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、前記画像データに対し、各種の画像処理を施す画像編集部と、前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第２の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部とからなる。

【００１４】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。図１は本発明の第１実施形態に係るデジタル証拠カメラシステムの構成を示す図であり、デジタル証拠カメラ１００と改竄検査装置１０１とから構成される。デジタル証拠カメラ１００のカメラ部５０－１は、撮影レンズ１と、撮像素子２と、増幅器３と、Ａ／Ｄ変換器４と、信号処理部５とからなる撮像手段６０を有する。撮影レンズ１を介して入射した被写体像は撮像素子２により撮像される。この撮像により得られた電気信号は増幅器３により増幅され、Ａ／Ｄ変換部４でデジタル信号に変換されて信号処理部５で所定の信号処理が施された後、画像データとして画像メモリ６に記憶される。この画像メモリ６に記憶されている画像データは必要に応じて画像表示部７に表示される。

【００１５】画像メモリ６に記憶されている画像データはファイルフォーマット変換部８において、ＪＰＥＧ、ＴＩＦＦなどの標準の画像フォーマットに変換される。これにより、画像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図２の（Ａ））。次にＭＤ作成部９では、画像データあるいはヘッダをも含めた全体のデータに対してハッシュ関数などの所定の関数を適用することによりＭＤを作成する（図２の（Ｂ））。次に、ＭＡＣ作成部１１では、秘密鍵メモリ１０にあらかじめ記憶された秘密鍵$K_{private}$（カメラ）を用いてＭＤを暗号化することによりＭＡＣを作成する（図２の（Ｃ））。次に、ヘッダ記録部１１では、作成したＭＡＣを画像ヘッダ中に格納する（図２の（Ｄ））。ファイリング管理部１３ではこのようにして作成されたファイルフォーマットの画像ファイルに対するファイル管理を行う。

【００１６】このような画像ファイルが記憶媒体制御部１５の制御により取外し可能な記憶媒体１７に記憶されて持ち運ばれる間に、あるいは通信制御部１４の制御により通信回線１６を介して送信される途中で改竄されたか否かを検知するために、改竄検知装置１０１が用いられる。

【００１７】すなわち、改竄検査装置１０１に装着された記憶媒体１７に記憶されている画像ファイルは、記憶媒体制御部１８の制御によりファイリング管理部１９に読み出される。あるいは、当該画像ファイルは通信制御部２４の制御により通信回線２５を介してファイリング管理部１９へと送られる。ファイリング管理部１９では、画像ファイルがＭＡＣと画像データ（この画像データには、画像データそのものの他に、ＪＰＥＧやＴＩＦＦ等のヘッダー情報を含めてもよい）とに分離され、ＭＡＣは復号化部２１に入力され、画像データはＭＤ作成部２２に入力される。

【００１８】復号化部２１では公開鍵メモリ２０にあらかじめ記憶されている公開鍵K_{public}（カメラ）を用いてＭＡＣを復号化することによりＭＤ１を生成する。この公開鍵K_{public}（カメラ）と前記した秘密鍵$K_{private}$（カメラ）とは、暗号化／復号化処理においてペアとなる鍵である。一方、ＭＤ作成部２２では入力された画像データからハッシュ関数などの所定の関数を用いてＭＤ２を生成する。次に、比較一致部２３ではＭＤ１とＭＤ２とを比較して両者が一致しなかった場合には画像ファイルが第３者により改竄されたと判定することができる。

【００１９】上記した第１実施形態によれば、画像データからカメラ内の暗号化鍵を用いて改竄検知用データ（ＭＡＣ）を作成し、この改竄検知用データを画像ファイル内、例えば画像のヘッダ情報内に書き込んでおくことで、画像データが改竄されているかどうかを確認できる。これにより、従来フィルムを用いて撮影された画像に比べ、劣るとされていたデジタル画像の証拠能力を高めることができる。

【００２０】また、改竄検知用データを作成するための暗号化鍵は、カメラ利用者を含め外部に絶対に漏洩することがあってはならないが、本実施形態では改竄検知用データを作成するための暗号化鍵は、あらかじめカメラ内のメモリ領域に格納されるため、暗号化鍵をハード的に極めて高いセキュリティレベルで管理できる。

【００２１】次に本発明の第２実施形態として、各種のモード（マルチモード）を有するデジタル証拠カメラについて説明する。ここでは、カメラに以下の各種モードの選択機能を備えることで、カメラの使用目的に応じた所望の機能を設定できる。ここで各種モードとは、セキュリティ機能を働かせない通常の撮影モード、撮影した画像ファイルに改竄検知データを付与する改竄監視モード、また、撮影した写真の著作権情報を画像ファイルに

電子透かしとして記録する電子透かしモード、さらには画像ファイルを取り外し可能な記憶媒体に保存する場合、あるいは通信機能を用いて画像ファイルを送信する場合に画像ファイルを暗号化するセキュアモード、等である。

【００２２】以下、図３を参照してさらに詳細に説明する。図３において図１と同一の参照番号を有するものは同一の機能を有するものとする。この実施形態におけるカメラ部５０－２からなるデジタル証拠カメラ１０２において、使用者はモード選択部３１で上記した各種のモードのうちから所望のモードを選択することができる。

【００２３】例えば、ノーマルモードを選択したときには、撮像手段６０により被写体を撮像して得られた画像データが画像メモリ６に記憶される。このモードでは特にセキュリティモードは働かず、画像メモリ６から読み出された画像データはファイルフォーマット変換部８でフォーマット変換されてファイリング管理部１３に送られてファイル管理される。

【００２４】また、電子透かしモードを選択した場合には、画像データがファイルフォーマット変換部８から電子透かし作成部３０に入力されて当該画像データに電子透かしデータが埋め込まれた後、ファイルフォーマット変換部８に再び戻されてフォーマットの変換が行われ、ファイリング管理部１３でファイル管理される。

【００２５】また、改竄防止モードを選択した場合には、図２を参照して前記した方法でヘッダにＭＡＣが付加された後、ファイリング管理部１３にてファイル管理される。

【００２６】また、改竄検知モードが選択された場合には、記憶媒体１７あるいは通信回線１６を介して外部装置（ＰＣ、改竄検査装置など）から取得されてファイリング管理部１３に送られた画像ファイルに対する改竄の有無の検知が行われる。すなわち、ＭＡＣが付加された画像データはＭＡＣと画像データとに分離され、画像データはファイリング管理部からＭＤ作成部３３に入力され、ＭＡＣは復号化部３４に入力される。ＭＤ作成部３３では入力された画像データからハッシュ関数などの所定の関数を用いてＭＤを生成する。また、復号化部３４は公開鍵メモリ３５に記憶されている公開鍵K_{public}（カメラ）を用いてＭＤ'を生成する。比較一致部３２はＭＤとＭＤ'とを比較して一致するか否かを判断する。両者が一致しなかった場合には画像データが第３者により改竄されたことがわかる。

【００２７】また、セキュアモードは画像データを記憶媒体に記憶するときに用いられる。この場合には、ファイリング管理部１３から画像データが読み出されて暗号化部３６に入力される。暗号化部３６はこの画像データを共有鍵メモリ３７に記憶されている共有鍵を用いて暗号化し、暗号化した画像データを再度ファイリング管理部１３に送る。この後、記録媒体制御部１５の制御によりこの暗号化された画像データが取外し可能な記憶媒体１７に書き込まれる。

【００２８】また、セキュアモードは通信回線を介して画像ファイルを伝送するときにも用いられる。この場合には、ファイリング管理部１３から画像データが読み出されて暗号化部３６に入力される。暗号化部３６はこの画像データを共有鍵メモリ３７に記憶されている共有鍵を用いて暗号化し、暗号化した画像データを通信制御部１４の制御により通信回線１６を介して外部装置（ＰＣ、改竄検査装置など）に送信する。

【００２９】上記した第２実施形態によれば、例えば、スナップ画像を撮る時にはノーマルモードで撮影し、証拠画像となるものを撮影する場合には改竄監視モード、また、著作権を守りたい画像に対しては電子透かしモードで撮影することで著作権を守ることができる。さらに、機密性の高い画像を撮影し、画像ファイルを安全に送信したい場合には、セキュアモードを選択することで、データの保存や送信を安全に行うことができる。また、複数のモードを組み合わせることで上記の効果から、１台のカメラを様々な用途に利用することが可能となる。

【００３０】以下に図４を参照して本発明の第３実施形態を説明する。図４において、図１と同様の参照数字のものは同様の機能を有するものとする。また、ここでは図１の通信機能及び図３の各種モードの構成を省略しているが、これらの機能を備えていても良いことは勿論である。カメラ部５０－３を有するデジタル証拠カメラ１０３において、撮像手段６０によって被写体を撮像することによって得られた画像データは画像メモリ６に記憶される。画像メモリ６から画像データがファイルフォーマット変換部８に読み出されて、ＪＰＥＧ、ＴＩＦＦなどの標準の画像フォーマットに変換される。これにより、画像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図５の（Ａ））。

【００３１】同時に、ＩＣカード制御部４１の制御によりカメラ部５０－３に装着された個人認証用ＩＣカード４０から個人認証用の情報が読み出されてファイルフォーマット変換部８に入力されて、ヘッダに個人認証用の情報が図５の（Ｂ）に示すように記録される。次にＭＤ作成部９では、データ全体、もしくは画像データ及び個人認証用データに対してハッシュ関数などの所定の関数を適用することによりＭＤを作成する（図５の（Ｃ））。次に、ＭＡＣ作成部１１では、秘密鍵メモリ１０にあらかじめ記憶された秘密鍵$K_{private}$（カメラ）を用いてＭＤを暗号化することによりＭＡＣを作成する（図５の（Ｄ））。ヘッダ記録部１２では、画像ヘッダ中に画像ヘッダ情報のデータ及び個人認証用データに加えて、ＭＡＣを格納する。これにより、画像ファイルは図５の（Ｅ）に示すような画像フォーマットでファイリング管理部１３に保存されてファイル管理される。

【００３２】このような画像ファイルが記憶媒体制御部１５の制御により取外し可能な記憶媒体１７に記憶されて持ち運ばれる間に改竄されたか否かを検知するために、改竄検知装置１０４が用いられる。

【００３３】すなわち、改竄検査装置１０４に装着された記憶媒体１７に記憶されている画像ファイルは、記憶媒体制御部１８の制御によりファイリング管理部１９に読み出される。ファイリング管理部１９では、画像ファイルがＭＡＣと前記したＭＡＣを求めるのに必要なデータ、すなわちＭＡＣを除くデータ全体、もしくは画像データ（この画像データには、画像データそのものの他に、ＪＰＥＧやＴＩＦＦ等のヘッダ情報を含めてもよい）及び個人認証用データ、とに分離され、ＭＡＣは復号化部２１に入力され、ＭＡＣを求めるのに必要なデータはＭＤ作成部２２に入力される。さらに個人認証用データは個人情報読み出し部２２にも入力される。

【００３４】復号化部２１では公開鍵メモリ２０にあらかじめ記憶されている公開鍵K_{public}（カメラ）を用いてＭＡＣを復号化することによりＭＤ１を生成する。一方、ＭＤ作成部２２では入力された画像データからハッシュ関数などの所定の関数を用いてＭＤ２を生成する。次に、比較一致部２３ではＭＤ１とＭＤ２とを比較して両者が一致しなかった場合には第３者により改竄されたと判定することができる。

【００３５】また、個人情報読み出し部４２では個人認証用データを読み出すことにより撮影者の特定が行われる。ここで、撮影者の特定は、画像データが改竄されていないことが確認された場合にのみ意味がある。

【００３６】上記した第３実施形態によれば、画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。特に、ここでは、撮影者の個人認証用の情報として、画像データと個人認証用データを合わせたデータから、前記暗号化鍵を用いて改竄検知用データを作成しているので、１つの改竄検知データで、画像データの改竄と撮影者の個人認証用データの改竄を検知できる。撮影者の個人認証用データが改竄されてなければ、個人認証用データから撮影者を特定できる。

【００３７】以下に本発明の第４実施形態を説明する。図６において、図１と同様の参照数字のものは同様の機能を有するものとする。また、ここでは図１の通信機能及び図３の各種モードの構成を省略しているが、これらの機能を備えていても良いことは勿論である。カメラ部５０－４を有するデジタル証拠カメラシステム１０５において、撮像手段６０によって被写体を撮像することによって得られた画像データは画像メモリ６に記憶される。画像メモリ６から画像データがファイルフォーマット変換部８に読み出されて、ＪＰＥＧ、ＴＩＦＦなどの標準の画像フォーマットに変換される。これにより、画像データにヘッダ情報のデータが付加されたファイルフォーマットが作成される（図７の（Ａ））。次にＭＤ作成部９においてデータ全体、もしくは画像データからハッシュ関数などの所定の関数を用いてＭＤ１あるいはＭＤ２（図７の（Ｂ）、（Ｂ）’）を生成する。このＭＤ１とＭＤ２とは同一のものであってもよい。ＭＤ１はＭＡＣ作成部１１に入力される。ＭＡＣ作成部１１では秘密鍵メモリ１０にあらかじめ記憶されている秘密鍵$K_{private}$（カメラ）を用いてＭＡＣを計算してＭＡＣ１を作成する（図７の（Ｃ））。このＭＡＣ１はヘッダ記録部１２に送られる。

【００３８】一方、ＭＤ２はＩＣカード制御部４１を介して、カメラ部５０－４に装着された個人認証用ＩＣカード４０’に入力される。個人認証用ＩＣカード４０’では、内部の秘密鍵メモリに記憶されている秘密鍵$K_{private}$（ＩＣカード）を用いてＭＤ２を暗号化してＭＡＣ２を作成する（図７の（Ｃ）’）。このＭＡＣ２は、ＩＣカード制御部４１を介してヘッダ記録部１２に送られる。

【００３９】ヘッダ記録部１２では、画像ヘッダ中に、画像ヘッダ情報のデータに加えて、ＭＡＣ１とＭＡＣ２とを格納する。これにより、画像ファイルは図７の（Ｄ）に示すような画像フォーマットでファイリング管理部１３に保存されてファイル管理される。

【００４０】このような画像ファイルが記憶媒体制御部１５の制御により取外し可能な記憶媒体１７に記憶されて持ち運ばれる間に改竄されたか否かを検知するために、改竄検知装置１０６が用いられる。

【００４１】すなわち、改竄検査装置１０６に装着された記憶媒体１７に記憶されている画像ファイルは、記憶媒体制御部１８の制御によりファイリング管理部１９に読み出される。

【００４２】ファイリング管理部１９では、画像ファイルがＭＡＣ１、ＭＡＣ２と画像データ（この画像データには、画像データそのものの他に、ＪＰＥＧやＴＩＦＦ等のヘッダー情報を含めてもよい）とに分離され、ＭＡＣ１は復号化部２１－１に入力され、画像データはＭＤ作成部２２－１に入力される。復号化部２１－１では公開鍵メモリ２０’にあらかじめ記憶されている公開鍵K_{public}（カメラ）を用いてＭＡＣ１を復号化することによりＭＤ１を生成する。公開鍵K_{public}（カメラ）と秘密鍵$K_{private}$（カメラ）とは、暗号化／復号化処理においてペアとなる鍵である。一方、ＭＤ作成部２２－１では入力された画像データからハッシュ関数などの所定の関数を用いてＭＤ１’を生成する。次に、比較一致部２３－１ではＭＤ１とＭＤ１’とを比較して両者が一致しなかった場合には第３者により改竄されていると判定することができる。

【００４３】同様にして、ＭＡＣ２は復号化部２１－２に入力され、画像データはＭＤ作成部２２－２に入力さ

れる。復号化部２１－２では公開鍵メモリ２０'にあらかじめ記憶されている公開鍵K_{public}（ＩＣカード）を用いてＭＡＣ２を復号化することによりＭＤ２を生成する。公開鍵K_{public}（ＩＣカード）と秘密鍵$K_{private}$（ＩＣカード）とは、暗号化／復号化処理においてペアとなる鍵である。

【００４４】一方、ＭＤ作成部２２－２では入力された画像データからハッシュ関数などの所定の関数を用いてＭＤ2'を生成する。次に、比較一致部２３－２ではＭＤ２とＭＤ２'とを比較して両者が一致したときには撮影者を特定することができる。

【００４５】上記した第４実施形態によれば、画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。特に、ここでは、撮影者の個人認証用の情報として、カメラ外部の装置で作成した第２の改竄検知用データを用いているので、第２の改竄検知用データとして電子メールや電子商取引など他の情報システムで用いられている電子署名を応用することが可能である。したがって、電子公証局や電子商取引などの社会基盤的な情報システムと連携が取れたデジタル証拠カメラシステムを構築することもできる。

【００４６】以下に、本発明の第５実施形態を説明する。第５実施形態は例えばボード、ＰＣＭＣＩＡカード等のハードウェアにて構成したイメージサーバを用いたデジタル画像編集システムに関するものである。ここでは説明を簡単にするためにイメージサーバの最小限の構成を想定する。

【００４７】従来、文書データに対して用いられている改竄検知用データを用いる方法では、オリジナルデータをほんのわずかでも改変すると改竄されたと見なされた。しかし、画像データに関してはデータの性質上、圧縮や切り抜き、キャプションの挿入等の処理が必要になる場合が多い。フィルムを用いた写真の場合であれば、必要な部分だけ印画紙に焼き付けたり、写真の裏にコメントを記述することに相当する。正当な理由があれば、このような処理は改竄にあたらない。正当な処理がなされたかどうかを判断できるようにするための方法としては、オリジナル画像データにどのような処理が施されたのか、その処理履歴を記録する方法がある。

【００４８】本実施形態では、イメージサーバを用いることで、画像データの圧縮、一部の領域の切り抜き、キャプションの追加などの処理を施した画像には、施した処理の履歴とともに、イメージサーバ以外で改竄されているかどうかを検知するようにする。

【００４９】図８は第５実施形態のイメージサーバシステム１０７の構成を示す図であり、例えば図１１に示すように、パソコン１０７－１と、このパソコン１０７－１に装着可能なＰＣＭＣＩＡカードからなるイメージサーバ１０７－２とから構成される。

【００５０】以下に第５実施形態の作用を図９のフローチャートを参照して説明する。まず、ファイリング管理部７２は、記憶媒体制御部７１の制御により記憶媒体７０から、図９の（Ａ）に示すようなフォーマットの画像ファイルを取得する。あるいは、外部装置９３から通信回線７７を介して通信制御部７８の制御により当該画像ファイルを取得する（ステップＳ１）。この場合、ファイリング管理部７２に直接接続可能な、シリアルケーブル、ＳＣＳＩ、ＩｒＤＡ等の接続端子を設けておくことで外部装置から容易に画像ファイルを入力することができる。また、イーサネット等のネットワーク接続の端子を備えた場合でも同様の効果が得られる。次に、ＭＡＣ検証部７３は、ファイリング管理部７２から画像ファイルを受け取ってＭＡＣ１を検証する（ステップＳ２）。すなわち、ファイリング管理部７２は画像ファイルをＭＡＣ１と画像データとに分離し、ＭＡＣ１は復号化部７５に入力され、画像データはＭＤ作成部７６に入力される。復号化部７５は公開鍵メモリ７４に記憶された公開鍵K_{public}（カメラ）を用いて復号化してＭＤ１を作成する。また、ＭＤ作成部７６はハッシュ関数などの所定の関数を用いてＭＤ１'を作成する。比較一致部７９はＭＤ１とＭＤ１'とを比較することにより、カメラで撮影された画像がその後改竄されているか否かに関する検証結果をファイリング管理部７２に送る。

【００５１】改竄されていない場合には、画像ファイルはファイリング管理部７２から画像編集部９３に入力されて画像編集ツール８０を用いたユーザによる画像編集が行われる（ステップＳ３）。この場合、画像ファイルの内容は画像表示装置８２に表示され、ユーザ９１はこの画面を見ながらデータ入力装置（キーボード、マウス等）８４を用いて各種の処理の要求を行ったり、データを入力する。８３はユーザ９１とイメージサーバ１０７とのユーザインタフェースである。編集時の履歴は編集履歴記録部８１に記録される。同時に、編集履歴記録部８１は、ＩＣカード制御部８５の制御により個人認証用ＩＣカード９２から個人認証用の情報を読み出して編集履歴中に記録する。上記編集はユーザから編集停止の指示が出されステップＳ５の判断がＮＯとなるまで継続される。

【００５２】編集後の画像ファイルと編集履歴のデータはファイリング管理部７２に送られるので、ファイリング管理部７２は編集履歴の情報を図９の（Ｂ）に示すようなフォーマットで画像ヘッダに記録する（ステップＳ６）。撮影したカメラを特定する情報を残す場合には、図９の（Ｃ）に示すようなフォーマットでカメラ情報も画像ヘッダに記録する。

【００５３】次に、編集後の画像ファイルと編集履歴のデータとがファイリング管理部７２から画像ファイル更新部８６のＭＤ作成部８７に入力されてハッシュ関数などの所定の関数を用いてＭＤ２が作成される。次に、Ｍ

ＡＣ作成部８８は秘密鍵メモリ９０にあらかじめ記憶されているイメージサーバ１０７の秘密鍵$K_{private}$（イメージサーバ）を用いてＭＤ２を暗号化することによりＭＡＣ２を作成する（ステップＳ７）。ヘッダ記録部８９ではこのＭＡＣ２を図９の（Ｄ）で示すようなフォーマットで画像ヘッダに記録する（ステップＳ８）。カメラを特定する情報を残す場合には図９の（Ｅ）に示すようなフォーマットになる。ＭＡＣ２が付加された画像ファイルはファイリング管理部７２に送られ、この後、この画像ファイルは、記憶媒体制御部７１の制御により取外し可能な記憶媒体７０に保存されるか、あるいは、通信制御部７８の制御により通信回線７７を介して外部装置９３に送られて保存される。

【００５４】上記した第５実施形態によれば、イメージサーバを用いることで、オリジナルの画像ファイルからどのような処理が施されたか、また、イメージサーバ以外で画像内容が変更されたかどうかを確認できるため、データ圧縮や領域切り出しのような、画像データの性質上必要な処理を施しても改竄とならない。また、イメージサーバで編集後に画像ファイルに付加する改竄検知用データを作成するときに、個人認証用データも用いることで、画像を編集したユーザを特定することができる。

【００５５】以下に、本発明の第６実施形態を説明する。第６実施形態は第５実施形態におけるイメージサーバをＰＣ等の上で起動されるソフトウェアにて構成したものである。ここでは説明を簡単にするためにイメージサーバの最小限の構成を想定する。

【００５６】図１０はイメージサーバをＰＣにインストールして構成されるイメージサーバシステム１０８の構成を示す図である。ここでは図８に示す第５実施形態の構成と異なる点についてのみ説明する。

【００５７】第６実施形態では図１０に示すように、ＭＡＣ作成部８８と、秘密鍵$K_{private}$が記憶された秘密鍵メモリ９０とが、イメージサーバシステム１０８の内部ではなく、イメージサーバ１０８に対して着脱自在なＩＣカード１０９の内部に設けられている。また、ＩＣカード制御部８５は、イメージサーバシステム１０８の画像ファイル更新部８６’の内部に設けられている。

【００５８】編集後の画像ファイルと編集履歴のデータとは画像ファイル更新部８６’のＭＤ作成部８７に入力されてハッシュ関数などの所定の関数を用いてＭＤ２が作成される。このＭＤ２はＩＣカード制御部８５の制御によりＩＣカード１０９のＭＡＣ作成部８８に送られる。ＭＡＣ作成部８８はＭＤ２を秘密鍵$K_{private}$（ＩＣカード）を用いて暗号化してＭＡＣ２を作成する。このＭＡＣ２はＩＣカード制御部８５の制御によりヘッダ記録部８９に送られて図９の（Ｄ）または（Ｅ）に示すようなフォーマットで画像ヘッダに記録される。なお、第５実施形態のようにＩＣカード１０９に個人認証用情報を格納しておき、これを読み出して編集履歴中に記録するようにしてもよい。

【００５９】上記した第６実施形態によれば、第５実施形態の効果に加えて、暗号化鍵の管理と暗号化の処理をＩＣカードのような着脱自在な記憶媒体で構成し、画像の編集や編集履歴データの作成などの他の機能をソフトウェアで構成するようにしたので、低コストでイメージサーバを構築できる効果を有する。

【００６０】以下に本発明の第７実施形態を説明する。第７実施形態は復号化鍵取得・登録システムに関し、公開鍵サーバ機構と改竄検査装置、イメージサーバの公開鍵取得・登録機構とから構成される。本実施形態で用いられる暗号化としての秘密鍵と復号化鍵としての公開鍵とは図１３（Ａ）に示すように、メーカーにより、デジタルカメラ２２０やイメージサーバ２２１、ＩＣカード２２２などの装置の製造時に鍵生成機構１２０により生成され、このうち、秘密鍵は装置に内蔵、登録される。登録後、この秘密鍵は直ちに安全かつ確実な方法で消去される。

【００６１】また、公開鍵は装置に固有の識別子としてのシリアル番号と対応させて図１３（Ｂ）に示す公開鍵サーバ機構１１０の鍵登録部２０２により記録媒体２０３に記憶される。

【００６２】改竄検知装置、イメージサーバの公開鍵取得・登録機構１１１が例えばデジタルカメラ２２０によって撮影された画像に対する改竄検知を行う場合には、公開鍵取得部２１２から装置のシリアル番号が通信制御部２１１、通信回線２１０、２０９、通信制御部２０８を介して鍵検索部２０４に送信される。鍵検索部２０４は装置のシリアル番号に対応する公開鍵を記憶媒体２０３から読み出してＭＤ作成部２０５に送る。ＭＤ作成部２０５はハッシュ関数等の所定の関数を用いてＭＤを作成してＭＡＣ作成部２０６に送る。ＭＡＣ作成部２０６は秘密鍵メモリ２０７にあらかじめ記憶されている秘密鍵を用いてＭＡＣを作成し、公開鍵とともに通信制御部２０８、通信回線２０９、通信回線２１０、通信制御部２１１を介して公開鍵取得部２１２に送る。公開鍵取得部２１２は取得した公開鍵と装置のシリアル番号とを公開鍵登録部２１４に送る。公開鍵登録部２１４は当該公開鍵と装置のシリアル番号とを公開鍵メモリ２１３に登録する。

【００６３】同時に、公開鍵取得部２１２から公開鍵のデータがＭＤ作成部２１６に、ＭＡＣが復号化部２１７に送られる。ＭＤ作成部２１６はハッシュ関数等の所定の関数を用いてこの公開鍵のデータからＭＤを作成する。復号化部２１７は公開鍵メモリ２１８に記憶されている鍵管理サーバの公開鍵K_{public}（鍵管理サーバ）を用いてＭＡＣを復号化することによりＭＤ’を作成する。比較一致部２１５はＭＤとＭＤ’とを比較して一致するか否かにより改竄を検知する。ここでのＭＡＣの検証は通信手段で得られたカメラやイメージサーバの公開

鍵が、正当な鍵管理サーバから取得されたものか、さらには、通信の途中で改竄されていないかを確認するのが目的である。

【００６４】なお、公開鍵サーバ１１０に登録されている公開鍵は郵送等の安全な手段でユーザに届けるようにしてもよい。上記した第７実施形態によれば、改竄検知用データの復号化鍵は復号化鍵（公開鍵）サーバに装置のシリアル番号を送ることで取得することができる。したがって、例えば復号化鍵サーバをインターネットから利用できる場合には、カメラのシリアル番号を元に世界中どこからでも改竄検知用データを取得することができる。

【００６５】以下に本発明の第８実施形態を説明する。第８実施形態は多重解像度画像の改竄防止に関するものである。ドキュメントファイルは一部を改変した場合、文章が繋がらなくなったり、意味が変化してしまい、元のファイルとは内容が異なってしまう。それに対して画像データは冗長性が高いため、解像度の変更など、多少の編集を行っても被写体は認識できることが多い。そのため、画像を利用する側では、撮影時の画像サイズでは必要以上の大きさであり解像度を落としたいことや不必要な部分が写っているため、必要な部分のみを切り出したいことがある。ところが、通常は改竄防止用イメージサーバを用意し、その内部で画像を編集してＭＡＣを再度付加しなくてはならない。

【００６６】そこで、第８実施形態では、上記の問題を解決するために、改竄防止カメラの画像を、多重解像度画像を保持するフォーマットで保存するようにする。図１４は本発明の第８実施形態の構成を示す図である。デジタル証拠カメラ部１１２において、撮像手段６０により被写体を撮像することにより得られた画像データは画像メモリ６に記憶される。次にこの画像データは画像縮小部３００に入力されて、複数種類の解像度の画像に変換される。このとき、ユーザがＭＡＣ作成解像度指示部３０２を通じて改竄を保証したい最小の解像度を指定すると、これがファイリング管理部１３を介してＭＤ作成部９に送られる。ＭＤ作成部９ではハッシュ関数などの所定の関数を用いてＭＤを作成する。

【００６７】一方、秘密鍵メモリ１０には、カメラ固有のデータメモリ３０１に記憶されたカメラ固有のデータと、ＩＣカード制御部４１の制御により個人認証用ＩＣカード４０から読み出した個人認証用の情報とから作成された秘密鍵が記憶されている。ＭＡＣ作成部１１ではこの秘密鍵を用いてＭＤ作成部９で作成されたＭＤを暗号化してＭＡＣを作成してファイリング管理部１３に送る。ファイリング管理部１３は複数種類の解像度の画像データを１つのファイルにまとめ、さらに上記の指定された解像度のデータから作成したＭＡＣを当該画像データに付加して記憶媒体制御部１５の制御により記憶媒体１７に保存する。

【００６８】図１６は本実施形態の画像データファイルについて説明するための図である。図１６に示すように、高解像度から低解像度への変換はあらかじめ規定しておく。ＭＡＣ作成解像度指示部３０２で指示された、改竄防止を保証する解像度のデータからＭＡＣを作成し、画像データのヘッダまたは別のＭＡＣ管理ファイルに記録する。

【００６９】一方、改竄検査装置１１３では、記憶媒体制御部１８の制御により記憶媒体１７からＭＡＣ及び画像データを読み出してファイリング管理部１９に送る。ファイリング管理部９ではＭＡＣを復号化部２１に、画像データを画像メモリ３０３に送る。復号化部２１では公開鍵を用いてＭＡＣを復号化することでＭＤ１を作成する。また、画像メモリ３０３に記憶された画像データは画像縮小部３０４で所定の縮小方法で縮小された後、ＭＤ作成部２２に送られてハッシュ関数などの所定の関数を用いてＭＤ２が作成される。一致比較部２３ではＭＤ１とＭＤ２とを比較することにより画像データが改竄されたか否かを判断する。

【００７０】以下に図１５を参照して本発明の第９実施形態について説明する。第９実施形態は多重解像度の画像を保持し、かつ、各解像度の画像は一定サイズの小ブロックを単位として格納されている画像フォーマットの改竄を防止することを意図している。この画像フォーマットで小ブロックを単位として格納している理由は、画像の一部を高速に参照できるようにするためである。

【００７１】デジタル証拠カメラ１１４の作用は上記したデジタル証拠カメラ１１２の作用と同じであるが、この実施形態では画像縮小・分割部３０５を有し、ここで複数の解像度の画像を作成するとともに、図１７に示すように一定の大きさのブロック単位に画像を分割する。ファイリング管理部１３では、各小ブロック毎にＭＡＣを作成し、小ブロック毎のヘッダにＭＡＣを書き込む。ＭＡＣ付きの画像ファイルは記録媒体制御部１５の制御により記憶媒体１７にオリジナル画像として記憶される。

【００７２】撮影時、画像の撮影範囲全体や解像度が必要ないユーザは、一般のＰＣ１１５内で編集ソフトウェア３０６を利用して記憶媒体１７から読み出したオリジナル画像から必要な部分の切り出しや必要な解像度の画像を作成する。ユーザは必要な画像部分の位置、サイズ、解像度などを編集パラメータ３０７として画像編集部３０６に入力する。ファイリング管理部１３では、対応する解像度の画像から、対応する位置の画像ブロックを抽出し、別の画像ファイルに保存する。

【００７３】改竄検知装置１１６により改竄を検査するときには、記憶媒体制御部１８の制御により記憶媒体１７からファイリング管理部１９に編集済み画像を読み出す。改竄検知部３０８では編集済み画像に対して改竄検知が行われる。このとき、もともと小ブロック毎に付加

されていたＭＡＣをそのまま新しいファイルに付加しておけば、改竄防止イメージサーバを用意しなくとも、ユーザは画像に証拠性を持たせたまま、画像の領域切り出しや解像度の変更といった編集作業を行うことができる。また、コントラスト強調、平滑化などのフィルタ処理を行う場合には、画素値そのものを変更せずに、フィルタ処理の手順を記録したデータを付加すれば、フィルタ処理画像に関してもオリジナル画像の保証が可能になる。

【００７４】なお、上記した具体的実施形態には以下のような構成の発明が含まれている。

１．カメラにより被写体を撮像して得られた画像データの改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、からなることを特徴とするデジタル証拠カメラシステム。

（作用効果）本発明によれば、画像データからカメラ内の暗号化鍵を用いて改竄検知用データを作成し、この改竄検知用データを前記暗号化鍵に対応する復号化鍵を用いて復号化することにより、画像データが改竄されているかどうかを確認できる。これにより、従来フィルムを用いて撮影された画像に比べ、劣るとされていたデジタル画像の証拠能力を高めることができる。

【００７５】また、改竄検知用データを作成するための暗号化鍵は、カメラ利用者を含め外部に絶対に漏洩することがあってはならないが、本発明では改竄検知用データを作成するための暗号化鍵は、あらかじめカメラ内に格納されているため、暗号化鍵をハード的に極めて高いセキュリティレベルで管理できる。

２．前記暗号処理部は、前記画像データに所定の関数を適用して得られたデータを前記暗号化鍵を用いて暗号化することにより前記改竄検知用データを作成することを特徴とする構成１記載のデジタル証拠カメラシステム。

（作用効果）画像データに対する改竄の程度が少なくても変化が大きく現れるように、所定の関数（例えばハッシュ関数）を適用して得られたデータに対して暗号化を行なうことにより改竄検知用データを作成したので、より確実に改竄検知を行なうことができる改竄検知用データを提供することができる。

３．前記改竄検知部は、前記画像データに前記所定の関数を適用して得られたデータと、前記改竄検知用データを前記復号鍵を用いて復号化して得られたデータとを比較することにより、前記画像データが改竄されたか否かを検知することを特徴とする構成２記載のデジタル証拠カメラシステム。

（作用効果）前記改竄検知用データを用いているので、より確実に改竄検知を行なうことができる。

４．前記暗号処理部は、前記暗号化鍵と、個人認証用データとに基づいて前記改竄検知用データを作成することを特徴とする構成１記載のデジタル証拠カメラシステム。

（作用効果）画像データの改竄検知用データ作成時に、個人認証用の情報も付加することで、画像の改竄の有無のみならず、画像撮影者も特定することができる。

５．前記暗号処理部は、前記画像データから、前記暗号化鍵を用いて第１の改竄検知用データを作成し、前記画像データから、前記個人認証用データを用いて第２の改竄検知用データを作成して、前記第１及び第２の改竄検知用データを合わせて前記改竄検知用データとすることを特徴とする構成４記載のデジタル証拠カメラシステム。

（作用効果）画像データから作成した第１の改竄検知用データと、撮影者の個人認証用データから作成した第２の改竄検知用データとをあわせて改竄検知用データとして用いるので、前記第２の改竄検知用データを電子メールや電子商取引など他の情報システムで用いられている電子署名と同様に応用することが可能であり、電子公証局や電子商取引などの社会基盤的な情報システムと連携が取れたデジタル証拠カメラシステムを構築することもできる。

６．前記個人認証用データ及び前記暗号化鍵を記憶する記憶部と、前記個人認証用データから第２の改竄検知用データを作成する第２の暗号処理部とを備え、この前記第２の暗号処理部を前記カメラに対して着脱自在に構成したことを特徴とする構成４記載のデジタル証拠カメラシステム。

（作用効果）個人認証用データと暗号化鍵を記憶し、第２の改竄検知用データを作成する第２の暗号処理部を、カメラに対して着脱自在な媒体（ＩＣカード等）に設けたことで、この媒体を携帯しておけば、普段利用していない他人のカメラを用いた場合でも、確実に個人の認証及び撮影した画像の改竄の有無を確認することができる。

７．前記暗号処理部は、前記画像データと前記個人認証用データとを合わせたデータから、前記暗号化鍵を用いて前記改竄検知用データを作成することを特徴とする構成４記載のデジタル証拠カメラシステム。

（作用効果）撮影者の個人認証用の情報として、画像データと個人認証用データを合わせたデータから、前記暗号化鍵を用いて改竄検知用データを作成する方法の場合には、１つの改竄検知データで、画像データの改竄と撮影者の個人認証用データの改竄を検知できる。撮影者の個人認証用データが改竄されてなければ、個人認証用データから撮影者を特定できる。

８．カメラにより被写体を撮像して得られた画像データ

の改竄を検知するデジタル証拠カメラシステムであって、被写体を撮像するための撮像部と、撮像により得られた画像データから、あらかじめ内蔵された暗号化鍵を用いて改竄検知用データを作成する暗号処理部と、を具備するカメラと、前記暗号化鍵に対応する復号化鍵を用いて前記改竄検知用データを復号化し、この復号化の結果に基づいて前記画像データが改竄されたか否かを検知する改竄検知部と、からなり、前記カメラは、前記画像データが改竄されたか否かを検知する改竄監視モードに加えて、前記カメラから前記改竄検知部へ転送される画像データに対する暗号化を行なうセキュアモードと、電子透かしデータを画像データに埋め込む電子透かしモードと、セキュリティ機能を働かせないで通常の撮影を行なうノーマルモードとを有し、これらのモードから少なくとも１つの所望のモードを選択するためのモード選択部を有することを特徴とするデジタル証拠カメラシステム。

（作用効果）カメラに各種モードの選択機能を備えることで、カメラの使用目的に応じた所望の機能を設定できる。例えば、スナップ画像を撮る時にはノーマルモードで撮影し、証拠画像となるものを撮影する場合には改竄監視モード、また、著作権を守りたい画像に対しては電子透かしモードで撮影することで著作権を守ることができる。さらに、機密性の高い画像を撮影し、画像ファイルを安全に送信したい場合には、セキュアモードを選択することで、データの保存や送信を安全に行うことができる。また、複数のモードを組み合わせることで上記の効果から、１台のカメラを様々な用途に利用することが可能となる。

９．装置に固有の識別子と、この識別子に対応して生成された第１の暗号化鍵に対応する第１の復号化鍵とをあわせて記憶する復号化鍵記憶部と、前記第１の復号化鍵に関する改竄検知用データを第２の暗号化鍵を用いて作成し、この改竄検知用データと前記第１の復号化鍵とあわせて出力する復号化鍵出力部と、を備えた復号化鍵サーバと、前記復号化鍵サーバから通信手段等を介して取得した前記第１の復号化鍵を記憶する復号化鍵記憶部と、前記第２の暗号化鍵に対応する第２の復号化鍵を用いて、通信手段等を介して前記復号化鍵サーバから供給された前記改竄検知用データを復号化し、この復号化の結果に基づいて前記第１の復号化鍵が改竄されたか否かを検知する改竄検知部と、を備えた復号化鍵取得部と、からなることを特徴とする復号化鍵取得・登録システム。

（作用効果）本発明によれば、改竄検知用データの復号化鍵は復号化鍵サーバに装置のシリアル番号を送ることで取得することができる。したがって、例えば復号化鍵サーバをインターネットから利用できる場合には、カメラのシリアル番号を元に世界中どこからでも改竄検知用データを取得することができる。

１０．画像データの改竄を検知するとともに、画像データの編集を行なうデジタル画像編集システムであって、画像入力部を介して入力された画像データをファイリング管理するファイリング管理部と、前記画像データにあらかじめ付与された第１の改竄検知用データを、この改竄検知用データを作成する際に用いた暗号化鍵に対応する復号化鍵を用いて復号化するとともに、この復号された第１の改竄検知用データと前記画像データとを比較することにより画像データの改竄状態を検知する改竄検知部と、前記画像データに対し、各種の画像処理を施す画像編集部と、前記画像編集部によって各種画像処理を施された編集済み画像データと前記画像編集部による編集履歴のデータから、前記暗号化鍵とは別の暗号化鍵を用いて第２の改竄検知用データを作成し、これを前記編集済み画像データに付加する画像ファイル更新部と、からなることを特徴とするデジタル画像編集システム。

（作用効果）本発明によれば、画像データと編集履歴とをあわせて改竄検知用データを作成しているので、元の画像に対しどのような編集処理が施されたのかを確認でき、さらに、当該システム以外で画像編集処理が施されているかどうかを検知することができる。

１１．前記画像ファイル更新部は、デジタル画像編集システムに対して着脱自在であり、前記個人認証情報及び前記別の暗号化鍵を記憶するとともに、前記個人認証情報に前記別の暗号化鍵を用いて前記第２の改竄検知用データを作成することを特徴とする構成１０記載のデジタル画像編集システム。

（作用効果）暗号化鍵の管理と暗号化の処理をICカードのような着脱自在な記憶媒体で、画像の編集や編集履歴データの作成などの他の機能をソフトウェアで構成することで、低コストでイメージサーバを構築できる。

１２．前記編集履歴に個人認証情報をあわせて記録したことを特徴とする構成９記載のデジタル画像編集システム。

（作用効果）画像編集履歴のデータも含めた画像データに、個人認証用の情報を含めることで、画像を編集した人物を特定することができる。

１３．前記画像入力部は、外部記憶媒体に記憶された画像データを、前記画像ファイリング部に直接接続（ケーブル、ＩｒＤＡ）、又は、通信回線を介して接続することにより入力することを特徴とする構成９記載のデジタル画像編集システム。

（作用効果）イメージサーバの画像ファイリング部に、シリアルケーブル、SCSI、IrDA等の直接接続の端子や、イーサネット等のネットワーク接続の端子を備えることで、外部装置から容易に画像ファイルを入力することができる。

１４．前記画像データは、解像度の互いに異なる複数の画像データを組にして記憶した多重解像度画像データであり、前記暗号処理部は、前記改竄検知用データを作成

するため、前記多重解像度画像データのなかから所望の解像度を有する少なくとも一つの画像データを選択する選択部を有することを特徴とする構成１又は１０記載のデジタル証拠カメラシステム。

（作用効果）記録時に改竄検知を保証する解像度を規定することにより、画像を利用するユーザーは撮影時の解像度に依存しないで所望の解像度画像を利用することが可能となる。

１５．前記画像データは、解像度の互いに異なる複数の画像データを組にして記憶した多重解像度画像データであり、前記多重解像度画像データ内の各画像データは、所定の小ブロックを単位として記憶されており、前記暗号処理部は、前記小ブロック単位で、前記改竄検知用データを作成することを特徴とする構成１又は１０記載のデジタル証拠カメラシステム。

（作用効果）小ブロック毎に改竄検知データを付加することにより、専用のサーバを用意することなく、切り抜きのような画像編集を行なった画像に対しても改竄検知をすることができる。

【００７６】

【発明の効果】本発明によれば、デジタル画像の証拠能力を高めることができ、暗号化鍵を極めて高いセキュリティレベルで管理することができるデジタル証拠カメラシステム、復号化鍵取得・登録システムを提供することができ、さらに、画像の性質上必要となる圧縮や領域切り出し、キャプションの挿入等の編集を施してもデジタル画像の証拠能力を保てるデジタル画像編集システムを提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図２】画像データにＭＡＣが付加されるまでの手順を示す図である。

【図３】本発明の第２実施形態に係るデジタル証拠カメラの構成を示す図である。

【図４】本発明の第３実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図５】画像データに個人認証用データとＭＡＣが付加されるまでの手順を示す図である。

【図６】本発明の第４実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図７】画像データにＭＡＣ１及びＭＡＣ２が付加されるまでの手順を示す図である。

【図８】本発明の第５実施形態に係るイメージサーバシステムの構成を示す図である。

【図９】第５実施形態の作用を説明するためのフローチャートである。

【図１０】本発明の第６実施形態に係るイメージサーバシステムの構成を示す図である。

【図１１】第５実施形態のイメージサーバシステムの構成例を示す図である。

【図１２】第６実施形態のイメージサーバシステムの構成例を示す図である。

【図１３】本発明の第７実施形態に係る復号化鍵取得・登録システムの構成を示す図である。

【図１４】本発明の第８実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

【図１５】本発明の第９実施形態に係るデジタル証拠カメラシステムの構成を示す図である。

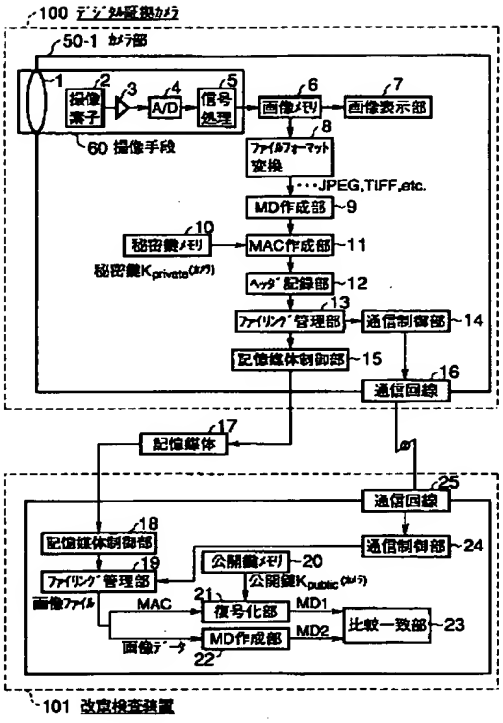
【図１６】第８実施形態に係る画像データファイルについて説明するための図である。

【図１７】第９実施形態に係る画像データファイルについて説明するための図である。

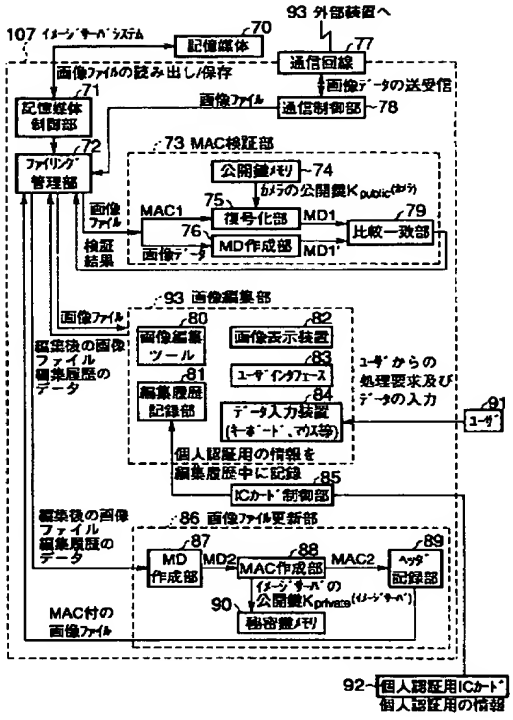
【符号の説明】

１…撮像レンズ、
２…撮像素子、
３…増幅部、
４…Ａ／Ｄ変換部、
５…信号処理部、
６…画像メモリ、
７…画像表示部、
８…ファイルフォーマット変換部、
９…ＭＤ作成部、
１０…秘密鍵メモリ、
１１…ＭＡＣ作成部、
１２…ヘッダ記録部、
１３…ファイリング管理部、
１４…通信制御部、
１５…記憶媒体制御部、
１６…通信回線、
１７…記憶媒体、
１８…記憶媒体制御部、
１９…ファイリング管理部、
２０…公開鍵メモリ、
２１…復号化部、
２２…ＭＤ作成部、
２３…比較一致部、
２４…通信制御部、
２５…通信回線、
５０－１…カメラ部、
６０…撮像手段、
１００…デジタル証拠カメラ、
１０１…改竄検査装置。

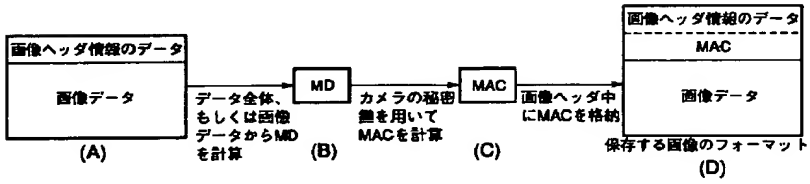
【図１】


100 デジタル証拠カメラ
50-1 カメラ部
1
2 撮像素子
3
4 A/D
5 信号処理
6 画像メモリ
7 画像表示部
60 撮像手段
8 ファイルフォーマット変換
・・・JPEG,TIFF,etc.
MD作成部 9
10 秘密鍵メモリ
秘密鍵$K_{private}$(カメラ)
MAC作成部 11
ヘッダ記録部 12
13 ファイリング管理部
通信制御部 14
記憶媒体制御部 15
16 通信回線
17 記憶媒体
通信回線 25
18 記憶媒体制御部
通信制御部 24
公開鍵メモリ 20
19 ファイリング管理部
公開鍵K_{public}(カメラ)
画像ファイル
MAC
21 復号化部
MD1
比較一致部 23
画像データ
MD作成部
MD2
22
101 改竄検査装置

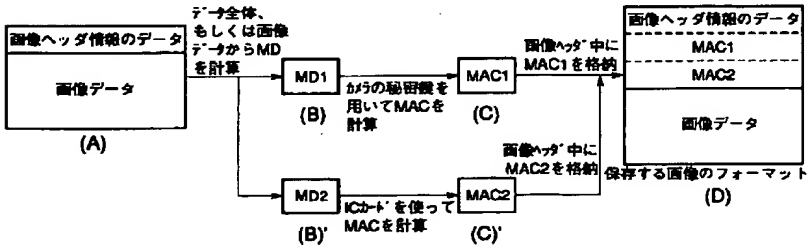
【図８】


93 外部装置へ
107 イメージサーバシステム
記憶媒体 70
通信回線 77
画像ファイルの読み出し/保存
画像データの送受信
記憶媒体制御部 71
画像ファイル
通信制御部 78
ファイリング管理部 72
73 MAC検証部
公開鍵メモリ 74
カメラの公開鍵K_{public}(カメラ)
画像ファイル
MAC1
75
復号化部
MD1
比較一致部 79
検証結果
76
画像データ
MD作成部
MD1'
93 画像編集部
画像ファイル
80 画像編集ツール
82 画像表示装置
83 ユーザインタフェース
編集後の画像ファイル編集履歴のデータ
81 編集履歴記録部
84 データ入力装置(キーボード、マウス等)
ユーザからの処理要求及びデータの入力
91 ユーザ
個人認証用の情報を編集履歴中に記録
85 ICカード制御部
編集後の画像ファイル編集履歴のデータ
86 画像ファイル更新部
87 MD作成部
MD2
88 MAC作成部
MAC2
89 ヘッダ記録部
イメージサーバの公開鍵$K_{private}$(イメージサーバ)
90 秘密鍵メモリ
MAC付の画像ファイル
92 個人認証用ICカード
個人認証用の情報

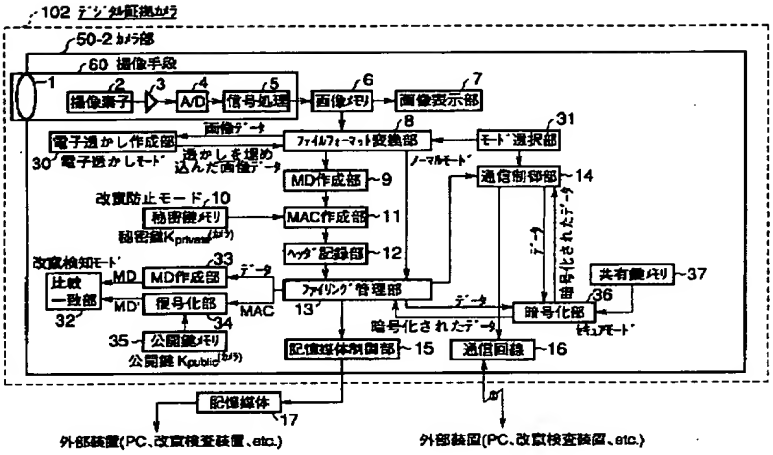
【図２】


画像ヘッダ情報のデータ
画像データ
(A)
データ全体、もしくは画像データからMDを計算
MD
(B)
カメラの秘密鍵を用いてMACを計算
MAC
(C)
画像ヘッダ中にMACを格納
画像ヘッダ情報のデータ
MAC
画像データ
保存する画像のフォーマット
(D)

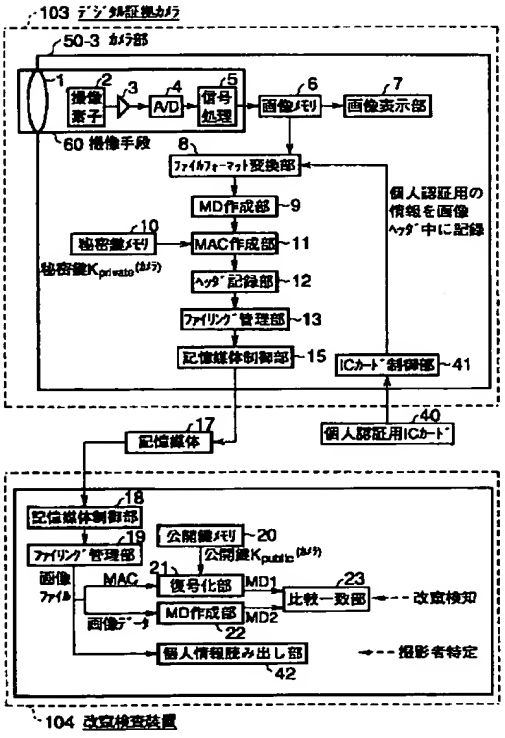
【図７】


画像ヘッダ情報のデータ
画像データ
(A)
データ全体、もしくは画像データからMDを計算
MD1
(B)
カメラの秘密鍵を用いてMACを計算
MAC1
(C)
画像ヘッダ中にMAC1を格納
MD2
(B)'
ICカードを使ってMACを計算
MAC2
(C)'
画像ヘッダ中にMAC2を格納
画像ヘッダ情報のデータ
MAC1
MAC2
画像データ
保存する画像のフォーマット
(D)

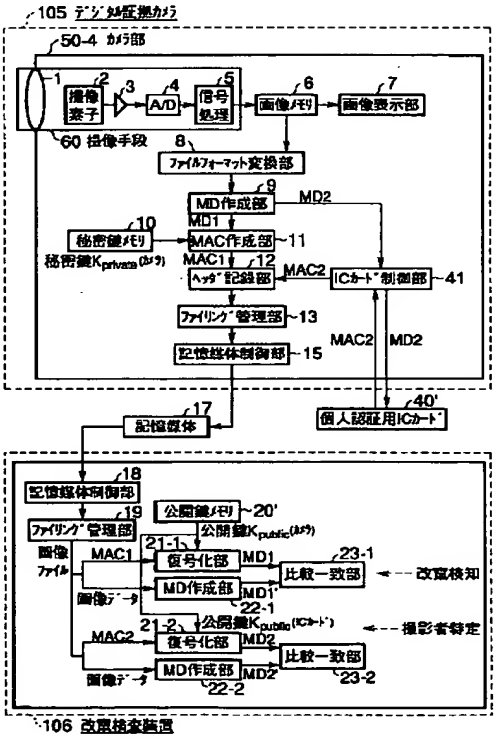
【図３】


102 デジタル証拠カメラ
50-2 カメラ部
60 撮像手段
撮像素子
A/D
信号処理
画像メモリ
画像表示部
ファイルフォーマット変換部
モード選択部
電子透かし作成部
電子透かしモード
透かしを埋め込んだ画像データ
ノーマルモード
MD作成部
通信制御部
改竄防止モード
秘密鍵メモリ
秘密鍵Kprivate(カメラ)
MAC作成部
ヘッダ記録部
改竄検知モード
比較一致部
復号化部
MD
MAC
データ
ファイリング管理部
暗号化部
暗号化されたデータ
共有鍵メモリ
公開鍵メモリ
公開鍵Kpublic(カメラ)
記憶媒体制御部
通信回線
記憶媒体
外部装置(PC、改竄検査装置、etc.)
外部装置(PC、改竄検査装置、etc.)

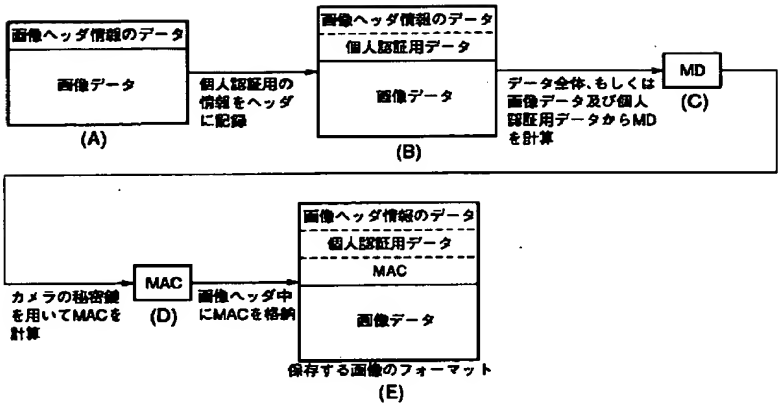
【図４】


103 デジタル証拠カメラ
50-3 カメラ部
60 撮像手段
撮像素子
A/D
信号処理
画像メモリ
画像表示部
ファイルフォーマット変換部
個人認証用の情報を画像ヘッダ中に記録
MD作成部
秘密鍵メモリ
秘密鍵Kprivate(カメラ)
MAC作成部
ヘッダ記録部
ファイリング管理部
記憶媒体制御部
ICカード制御部
記憶媒体
個人認証用ICカード
104 改竄検査装置
公開鍵メモリ
公開鍵Kpublic(カメラ)
画像ファイル
MAC
復号化部
MD1
比較一致部
改竄検知
MD作成部
MD2
画像データ
個人情報読み出し部
撮影者特定

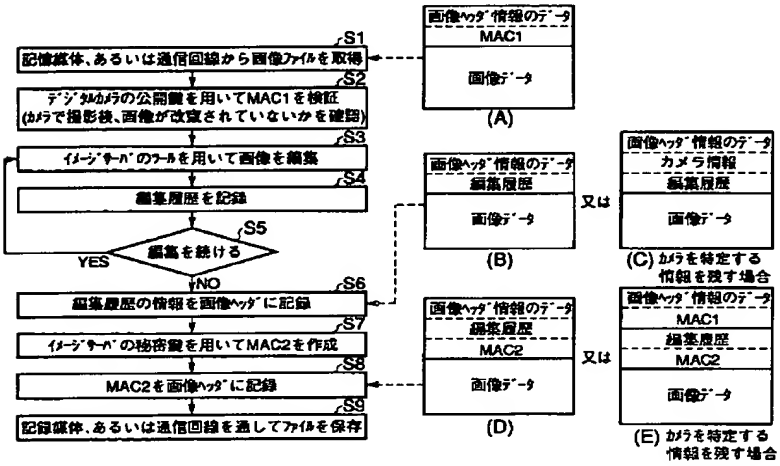
【図６】


105 デジタル証拠カメラ
50-4 カメラ部
60 撮像手段
撮像素子
A/D
信号処理
画像メモリ
画像表示部
ファイルフォーマット変換部
MD作成部
MD1
MD2
秘密鍵メモリ
秘密鍵Kprivate(カメラ)
MAC作成部
MAC1
ヘッダ記録部
MAC2
ICカード制御部
ファイリング管理部
記憶媒体制御部
記憶媒体
個人認証用ICカード
106 改竄検査装置
公開鍵メモリ
公開鍵Kpublic(カメラ)
画像ファイル
復号化部
比較一致部
改竄検知
画像データ
公開鍵Kpublic(ICカード)
撮影者特定

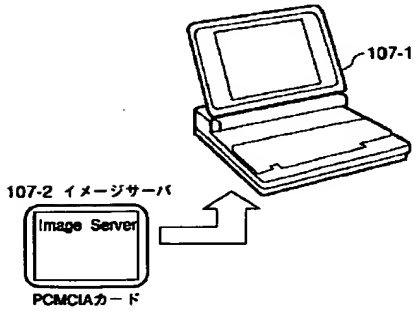
【図５】


画像ヘッダ情報のデータ
画像データ
(A)
個人認証用の情報をヘッダに記録
画像ヘッダ情報のデータ
個人認証用データ
画像データ
(B)
データ全体、もしくは画像データ及び個人認証用データからMDを計算
MD
(C)
カメラの秘密鍵を用いてMACを計算
MAC
(D)
画像ヘッダ中にMACを格納
画像ヘッダ情報のデータ
個人認証用データ
MAC
画像データ
保存する画像のフォーマット
(E)

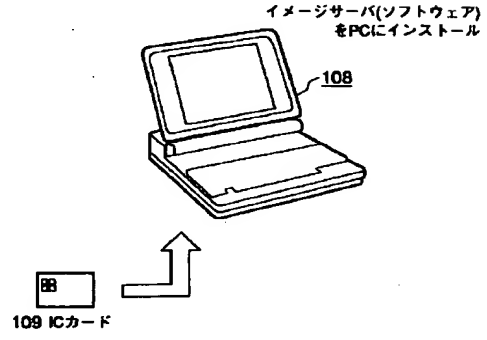
【図９】


S1
記憶媒体、あるいは通信回線から画像ファイルを取得
S2
デジタルカメラの公開鍵を用いてMAC1を検証
(カメラで撮影後、画像が改竄されていないかを確認)
S3
イメージサーバのツールを用いて画像を編集
S4
編集履歴を記録
S5
編集を続ける
YES
NO
S6
編集履歴の情報を画像ヘッダに記録
S7
イメージサーバの秘密鍵を用いてMAC2を作成
S8
MAC2を画像ヘッダに記録
S9
記録媒体、あるいは通信回線を通してファイルを保存
画像ヘッダ情報のデータ
MAC1
画像データ
(A)
画像ヘッダ情報のデータ
編集履歴
画像データ
(B)
又は
画像ヘッダ情報のデータ
カメラ情報
編集履歴
画像データ
(C) カメラを特定する情報を残す場合
画像ヘッダ情報のデータ
編集履歴
MAC2
画像データ
(D)
又は
画像ヘッダ情報のデータ
MAC1
編集履歴
MAC2
画像データ
(E) カメラを特定する情報を残す場合

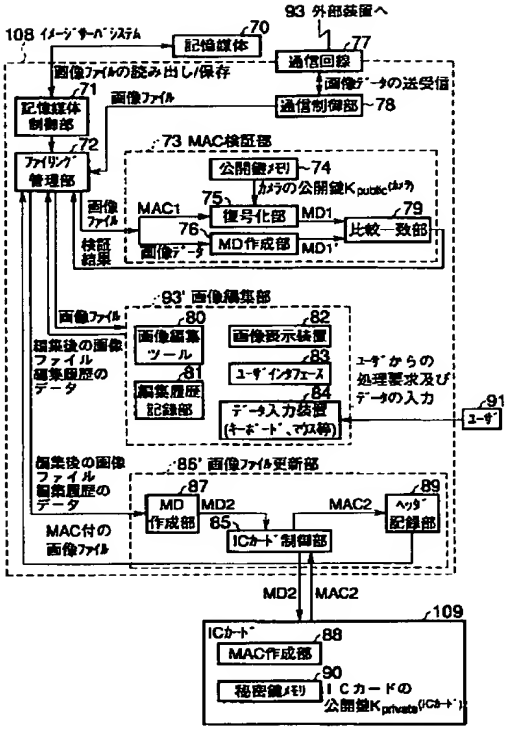
【図１１】


107-1
107-2 イメージサーバ
Image Server
PCMCIAカード

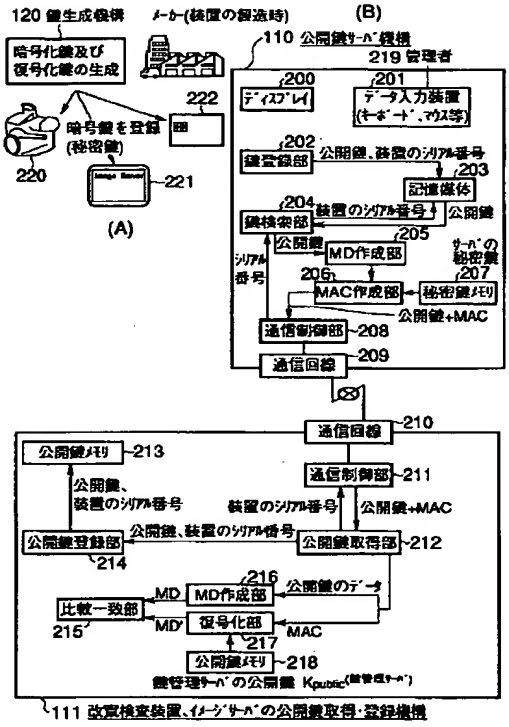
【図１２】


イメージサーバ(ソフトウェア)をPCにインストール
108
109 ICカード

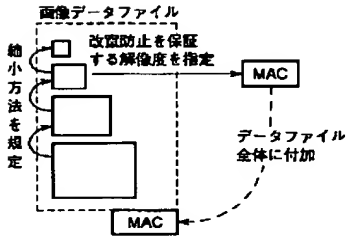
【図１０】



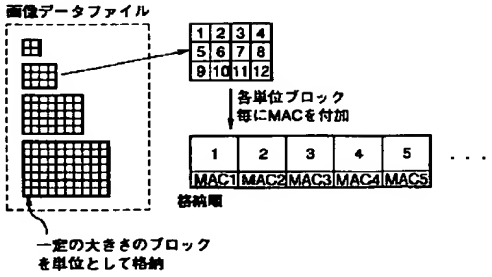
【図１３】



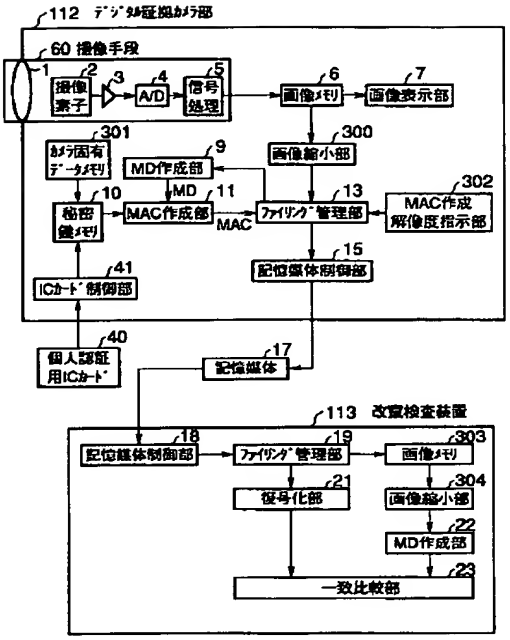
【図１６】



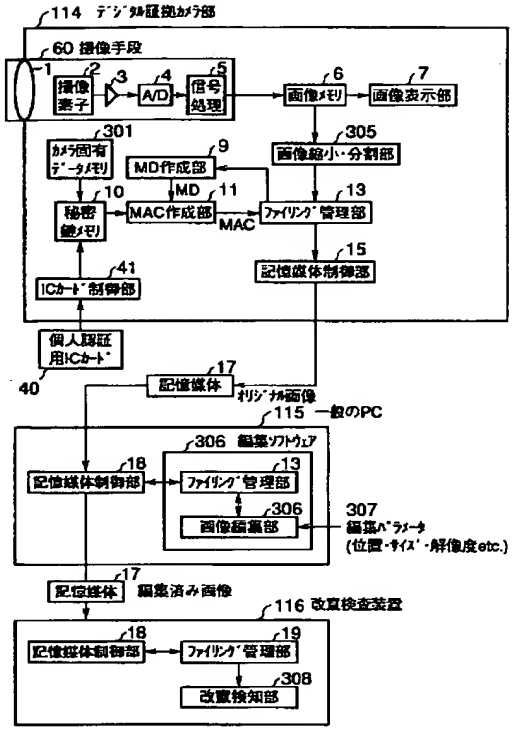
【図１７】



【図１４】



【図１５】



フロントページの続き

(72)発明者　山田　秀俊
東京都渋谷区幡ヶ谷２丁目43番２号　オリンパス光学工業株式会社内